UNITED STATES DISTRICT COURT

for the

Northern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

One cell phone, phone number 682-207-9322
Wireless provider T-Mobile, US, Inc.

Case No. 4:16-MJ-752

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment "A"

located in the Northern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252 and 2252A	Production, Distribution, Receipt and Possession of Child Pornography

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Kyle L. Kuykendall, Special Agent, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/6/16

Judge's signature

City and state: Fort Worth, Texas

United States Magistrate Judge Jeffrey L. Cureton
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Kyle L. Kuykendall, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to authorize law enforcement to employ an electronic investigative technique, which is described in Attachment B, to determine the location of the cellular device assigned call number **(682) 207-9322,** (the "Target Cellular Device"), which is described in Attachment A.

2. I am a Special Agent with the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and have been since August of 2008. As part of my duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have been involved in numerous child pornography investigations and am very familiar with the tactics used by child pornography offenders who collect and distribute child pornographic material.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. One purpose of applying for this warrant is to determine with precision the Target Cellular Device's location. There is reason to believe the Target Cellular Device is currently located somewhere within this district because on November 22, 2016, in the Northern District of Texas, I applied for and was granted a federal search warrant, compelling T-Mobile US, Inc., (the Target Cellular Device's service provider) to provide the E911 Phase 2 location data for the device. Since issuance and service of the search warrant on T-Mobile US, Inc., the Target Cellular Device has redominately emitted E911 Phase 2 location data indicating the device is located in the Northern District of Texas, specifically in the Wilmer-Hutchins area of Dallas County, Texas. While the E911 Phase 2 location data has identified the Target Cellular Device to be in the Northern District of Texas, the data received from T-Mobile US, Inc., has not been specific enough to isolate to the device to a single property or structure.

5. Pursuant to Rule 41(b)(2), law enforcement may locate the Target Cellular Device outside the district provided the device is within the district when the warrant is issued.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2252 and 2252A, that is offenses related to the production, distribution, receipt, and possession of child pornography have been committed, are being committed, and will be committed by the user of the cellular phone associated with the

number **(682) 207-9322**. There is also probable cause to believe that the location of the Target Cellular Device will constitute evidence of those criminal violations, including leading to the identification of individuals who are engaged in the commission of these offenses and identifying locations where the target engages in criminal activity.

7. Because collecting the information authorized by this warrant may fall within the statutory definitions of a "pen register" or a "trap and trace device," *see* 18 U.S.C. § 3127(3) & (4), this warrant is designed to comply with the Pen Register Statute as well as Rule 41. See 18 U.S.C. §§ 3121-3127. This warrant therefore includes all the information required to be included in a pen register order. See 18 U.S.C. § 3123(b)(1).

PROBABLE CAUSE

8. On November 20, 2015, in Indian Head Saskatchewan, Canada, a 14-year-old minor female victim contacted an investigator with the Royal Canadian Mounted Police (RCMP) to inform them that she had been the victim of extortion. She alleged that while utilizing the social media application "Kik Messenger" on her cellular phone, she entered into a conversation with an unknown person utilizing the username "**itsmeyall1**".

9. The user of "**itsmeyall1**" identified himself/herself as a fourteen-year-old female and encouraged the minor female victim to exchange photographs. The initial request was for images of the minor female victim's face, but subsequent requests progressed to explicit images of the minor female both in her underwear and with her genitals exposed. The user of "**itsmeyall1**" would respond by sending the minor female victim photographs of a similarly aged female engaging in similar behavior. During the conversations between the minor female victim and the user of "**itsmeyall1,**" the user of "**itsmeyall1**"

provided his/her phone number as **682-207-9322**. According to the minor female victim, "**itsmeyall1**" provided the number in the event that there was a problem with the KIK Messenger application and they needed an alternate means to communicate.

10. When the minor female victim grew tired of the conversation and decided to stop sending photographs of herself, the user of "**itsmeyall1**" threatened to post the explicit photos of the minor female victim to her personal Facebook page. The minor female victim then stopped all further communication with the user of "**itsmeyall1**" and deleted the Kik Messenger application from her cellular phone. The minor female victim indicated she sent approximately twenty-five (25) images and videos of herself to the user of "**itsmeyall1**".

11. In February of 2016, Constable Ken Samways, an officer with the RCMP sought and received a production order, pursuant to the Canadian Criminal Code, for the KIK Messenger service to provide subscriber information and stored content associated with the username "**itsmeyall1**". As a result of the production order served on the KIK Messenger service, the RCMP learned that the KIK Messenger user "**itsmeyall1**" had accessed the application from a cellular device, which was the assigned Internet Protocol (IP) address 172.56.6.240.

In response to the production order, KIK Messenger also provided fifty-one (51) folders of digital content sent or received by KIK user "**itsmeyall1**", many of which contain images depicting child pornography, as defined in 18 U.S.C. § 2256. Specifically, located in two of the above mentioned 51 folders, were images of the previously

referenced minor female victim engaged in sexually explicit conduct to include the lewd and lascivious exhibition of her genitals.

12. A commercial database search for the phone number **(682) 207-9322** indicates the service provider is T-Mobile US, Inc., doing business as Metro PCS. A search for the IP address 172.56.6.240 also resolved to T-Mobile US, Inc.

13. In April of 2016, an administrative summons was served on T-Mobile requesting subscriber information associated with phone number **(682) 207-9322**. The returned information identified the subscriber as Pedro De Pacas of [redacted] Hallmark Drive, in Arlington, Texas. The summons return also indicated the cellular phone number has been assigned to Pedro De Pacas since November 4, 2013. The return also identified three separate cellular devices have been associated with the phone number since the phone number has been assigned to Pedro De Pacas. A review of local property records and commercial databases indicate both the name and address identified in the T-Mobile summons return are fictitious.

14. In October of 2016, an administrative summons was served on KIK Messenger requesting IP logs for the previous sixty days for the user "**itsmeyall1.**" In response KIK Messenger provided logs indicating the application was most frequently accessed via T-Mobile/MetroPCS' wireless Internet service, which is consistent with the use of a MetroPCS "smart" cellular phone.

15. The KIK Messenger IP logs also indicated the KIK user "**itsmeyall1**" sporadically accessed the application from other Internet service providers, including an IP address associated with Charter Communications for approximately 20 minutes on October 14,

2016. Later the same day, the KIK user "**itsmeyall1**" accessed the application from an Internet protocol address resolving to Texas Health Resources for approximately two hours. Texas Health Resources is a network of 24 hospitals in the Dallas-Fort Worth area, which provide free wireless Internet access at many of their locations. Due to the KIK user's limited connection to these two Internet services, it is unlikely the two corresponding locations where the Internet was accessed are the KIK user's residence or place of employment.

16. On November 22, 2016, in the Northern District of Texas, I applied for and was granted a search warrant to be served on T-Mobile, which is the service provider for the Target Cellular Device. The search warrant compelled T-Mobile to provide E911 Phase 2 location data for the Target Cellular Device, which is the approximated near real-time latitude and longitude coordinates for the device.

Since issuance and service of the search warrant, the Target Cellular Device has emitted E911 Phase 2 information indicating it has been and is presently located in the Wilmer-Hutchins area of Dallas County, Texas. Though the information indicates the Target Cellular Device is presently in the Northern District of Texas, the approximated coordinates are not specific enough to identify the device's location to a singular property or structure.

17. Based on the aforementioned facts, I have reason to believe that the user of the Target Cellular Device has purposely obtained and continued service on a T-Mobile cellular device with a fictitious name and address for over three years for the specific purpose of engaging in ongoing criminal activity, namely the receipt and possession of

child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. Further, the user of cellular phone number, the Target Cellular Device, who is also believed to be the KIK user "**itsmeyall1**" has intentionally limited his/her Internet access for the KIK messenger application to the fictitiously registered T-Mobile account or functionally anonymous public Internet access points, for the purpose of masking his/her identity and avoiding detection by law enforcement.

MANNER OF EXECUTION

18. In my training and experience, I have learned that cellular phones and other cellular devices communicate wirelessly across a network of cellular infrastructure, including towers that route and connect individual communications.

When sending or receiving a communication, a cellular device broadcasts certain signals to the cellular tower that is routing its communication. These signals include a cellular device's unique identifiers.

19. To facilitate execution of this warrant, law enforcement may use an investigative device or devices capable of broadcasting signals that will be received by the Target Cellular Device or receiving signals from nearby cellular devices, including the Target Cellular Device. Such a device may function in some respects like a cellular tower, except that it will not be connected to the cellular network and cannot be used by a cell phone to communicate with others. The device may send a signal to the Target Cellular Device and thereby prompt it to send signals that include the unique identifier of the device. Law enforcement may monitor the signals broadcast by the Target Cellular

Device and use that information to determine the Target Cellular Device's location, even if it is located inside a house, apartment, or other building.

20. The investigative device may interrupt cellular service of phones or other cellular devices within its immediate vicinity. Any service disruption to non-target devices will be brief and temporary, and all operations will attempt to limit the interference with such devices. In order to connect with the Target Cellular Device, the device may briefly exchange signals with all phones or other cellular devices in its vicinity. These signals may include cell phone identifiers. The device will not complete a connection with cellular devices determined not to be the Target Cellular Device, and law enforcement will limit collection of information from devices other than the Target Cellular Device. To the extent that any information from a cellular device other than the Target Cellular Device is collected by the law enforcement device, law enforcement will delete that information, and law enforcement will make no investigative use of it absent further order of the court, other than distinguishing the Target Cellular Device from all other cellular devices.

AUTHORIZATION REQUEST

21. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41. The proposed warrant also will function as a pen register order under 18 U.S.C. § 3123.

22. I request this warrant be authorized for a period of 30 days, which will allow sufficient time to precisely locate the Target Cellular Device and conduct subsequent necessary investigative activity.

23. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days from the end of the period of authorized surveillance. This delay is justified because there is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the Target Cellular Device would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1).

There is reasonable necessity for the use of the technique described above, for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

24. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cellular Device outside of daytime hours.

25. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

26. A search warrant may not be legally necessary to compel the investigative technique described herein. Nevertheless, I hereby submit this warrant application out of an abundance of caution.

Respectfully submitted,

Kyle L. Kuykendall, Special Agent
Homeland Security Investigations

SWORN AND SUBSCRIBED before me, at 11:00 am/pm, this 6th day of December, 2016.

JEFFREY L. CURETON
United States Magistrate Judge

ATTACHMENT A

This warrant authorizes the use of the electronic investigative technique described in Attachment B to identify the location of the cellular device assigned phone number **(682) 207-9322,** whose wireless provider is T-Mobile US, Inc., and whose listed subscriber is unknown.

ATTACHMENT B

Pursuant to an investigation of identify of subject of investigation, for a violation of 18 U.S.C. §§ 2252 and 2252A, that is offenses related to the production, distribution, receipt, and possession of child pornography, this Warrant authorizes the officers to whom it is directed to determine the location of the cellular device identified in Attachment A by collecting and examining:

1. radio signals emitted by the target cellular device for the purpose of communicating with cellular infrastructure, including towers that route and connect individual communications; and
2. radio signals emitted by the target cellular device in response to radio signals sent to the cellular device by the officers;

for a period of thirty days, during all times of day and night. This warrant does not authorize the interception of any telephone calls, text messages, other electronic communications, and this warrant prohibits the seizure of any tangible property. The Court finds reasonable necessity for the use of the technique authorized above. *See* 18 U.S.C. § 3103a(b)(2).